ODLOČITVENI PROCES ZA IZBIRO PREMOSTITVENIH UKREPOV PROTI KIBERNETSKIM NAPADOM

Andrej Bregar (Informatika d.o.o.) Anas Husseis, Jose Luis Flores (IKERLAN)

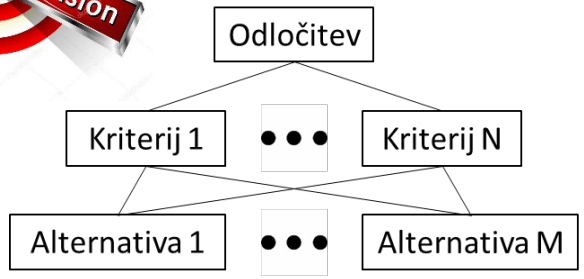
9. 5. 2023

Izhodišča

- Ena pomembnejših strategij v kibernetski varnosti so premostitveni ukrepi, s katerimi preprečimo učinke kibernetskih napadov in groženj ter povečamo splošno odpornost IT in OT infrastrukture.
- Cilj se je pripraviti na grožnje, oceniti njihov vpliv in postaviti prioritete glede pristopa ter ukrepov za njihovo omejevanje. Osnovni koncept ni izogibanje grožnjam in preprečevanje kibernetskih incidentov, temveč oblikovanje strategije, ki obravnava posledice incidenta ter vpelje zaporedje akcij, ki jih izvedemo še pred morebitnim varnostnim dogodkom, kar zmanjša kratkoročne in dolgoročne negativne učinke.
- Izbrati in implementirati je potrebno množico optimalnih premostitvenih ukrepov, s katerimi zagotovimo neprekinjenost poslovanja. Ker pomeni izvedba vsakega ukrepa strošek in ker utegne imeti ukrep zgolj omejen učinek, je potrebno upoštevati razmerje med ceno in učinkovitostjo posameznega ukrepa.
- Ključna je možnost izbire med pemostitvenimi ukrepi.
- Oceniti moramo primernost in učinkovitost vsakega potencialnega premostitvenega ukrepa na podlagi več kriterijev, ki upoštevajo značilnosti infrastrukture, zrelost razpoložljivih tehnologij in procesov za zagotavljanje kibernetske varnosti, organizacijske omejitve in cilje, resnost kibernetskih incidentov itd.
- Bistveno vlogo igra sistematičen in celovit odločitveni proces za ocenjevanje in izbiro premostitvenih ukrepov ali premostitvenih strategij.
- V sistemih kritične infrastrukture odraža izbira in implementacija premostitvenih ukrepov še dodatno dimenzijo kompleksnosti, saj so lahko številni IT in OT viri medsebojno povezani, hkrati pa več deležnikov zagotavlja skupne ključne storitve, si deli vire, sodeluje v dobavnih verigah itd. Zato je lahko v primeru prizadetosti enega vira zaradi kaskadnih učinkov kibernetskega napada ogroženih več povezanih virov.

Namen prispevka

- Namen je vzpostaviti metodologijo in proces večkriterijskega odločanja, ki na sistematičen in celovit način naslovi problem izbire in izvedbe premostitvenih ukrepov in premostitvenih strategij, ki omogočijo odziv na kibernetske incidente ter zmanjšujejo vpliv teh incidentov v kompleksnejših IT in OT sistemih.
- Pristop smo primarno vpeljali za elektroenergetsko kritično infrastrukturo, vendar je uporaben za vse organizacijske sisteme, ki so pri poslovanju zaradi digitalizacije izpostavljeni kibernetskim grožnjam.
- Odločitveno metodologijo smo razvili v sklopu mednarodnega razvojno-raziskovalnega projekta Horizon 2020 CyberSEAS, katerega cilj je vpeljava mehanizmov za povečanje odpornosti energetskega sistema.



CyberSEAS

Cyber Securing Energy dAta Services

https://cyberseas.eu/

Ogrodje za promostitvene ukrepe

MITRE | ATT&CK® Matrices Tactics Techniques Data Sources Mitigations Groups Software Campaigns Resources Blog Contribute
Search

ATT&CK v13 has been released! Check out the blog post or release notes for more information.

MITIGATIONS
- Enterprise
  - Account Use Policies
  - Active Directory Configuration
  - Antivirus/Antimalware
  - Application Developer Guidance
  - Application Isolation and Sandboxing
  - Audit
  - Behavior Prevention on Endpoint
  - Boot Integrity
  - Code Signing

Home > Mitigations > Enterprise

Enterprise Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

Mitigations: 43

ID	Name	Description
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M1015	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.
M1049	Antivirus/Antimalware	Use signatures or heuristics to detect malicious software.

CIS Controls v8 - (153) Show Version 7.1

	Sub	Title	Asset Type	Implementation Group:	IG1	IG2	IG3
CIS Control 1 - Inventory and Control of Enterprise Assets							
		Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devic connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.					
☑	1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Devices		●	●	●
☑	1.2	Address Unauthorized Assets	Devices		●	●	●
☑	1.3	Utilize an Active Discovery Tool	Devices			●	●
☑	1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Devices			●	●
☑	1.5	Use a Passive Asset Discovery Tool	Devices				●

DEFEND™
A knowledge graph of cybersecurity countermeasures
0.12.0-BETA-2

ATT&CK Lookup | Search D3FEND's 521 Artifacts | D3FEND Lookup

Model	Harden				Detect							Isolate		Dece
+	Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	Decoy Environment
	Application Configuration Hardening	Biometric Authentication	Message Authentication	Bootloader Authentication	Dynamic Analysis	Homoglyph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	Firmware Behavior Analysis	Database Query String Analysis	Authentication Event Thresholding	Executable Allowlisting	Broadcast Domain Isolation	Connected Honeynet
	Dead Code Elimination	Certificate-based Authentication	Message Encryption	Disk Encryption	Emulated File Analysis	Identifier Activity Analysis	Sender Reputation Analysis	Byte Sequence Emulation	Firmware Embedded Monitoring Code	File Access Pattern Analysis	Authorization Event Thresholding	Executable Denylisting	DNS Allowlisting	Integrated Honeynet
	Exception Handler Pointer Validation	Certificate Pinning	Transfer Agent Authentication	Driver Load Integrity Checking	File Content Rules	Identifier Reputation Analysis		Certificate Analysis	Firmware Verification	Indirect Branch Call Analysis	Credential Compromise Scope Analysis	Hardware-based Process Isolation	DNS Denylisting	Standalone Honeynet
	Pointer Authentication	Credential Rotation		File Encryption	File Hashing	Domain Name Reputation		Active Certificate	Peripheral Firmware	Process Code	Domain	IO Port Restriction	Forward Resolution Domain Denylisting	Decoy Public Releas

Strategies to Mitigate Cyber Security Incidents
ACSC Australian Cyber Security Centre
Last Updated: February 2017. First published February 2010.

Suggested Mitigation Strategy Implementation Order (start with threats of most concern to the organisation)

Targeted cyber intrusions (advanced persistent threats) and other external adversaries who steal data:
1. Implement 'essential' mitigation strategies to:
   a. prevent malware delivery and execution
   b. limit the extent of cyber security incidents
   c. detect cyber security incidents and respond.
2. Repeat step 1 with 'excellent' mitigation strategies.
3. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Ransomware and external adversaries who destroy data and prevent computers/networks from functioning:
1. Implement 'essential' mitigation strategies to:
   a. recover data and system availability
   b. prevent malware delivery and execution
   c. limit the extent of cyber security incidents
   d. detect cyber security incidents and respond.
2. Repeat step 1 with 'excellent' mitigation strategies.
3. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Note that 'Hunt to discover incidents' is less relevant for ransomware that immediately makes itself visible.

Relative Security Effectiveness	Mitigation Strategy	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Mitigation Strategies to Prevent Malware Delivery and Execution:				
Essential	**Application control** to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.	Medium	High	Medium
Essential	**Patch applications** (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computers with 'extreme risk' security vulnerabilities within 48 hours. Use the latest version of applications.	Low	High	High
Essential	**Configure Microsoft Office macro settings** to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.	Medium	Medium	Medium
Essential	**User application hardening**. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.	Medium	Medium	Medium
Excellent	**Automated dynamic analysis of email and web content run in a sandbox**, blocked if suspicious behaviour is identified (e.g. network traffic, new or modified files, or other system configuration changes).	Low	High	Medium
Excellent	**Email content filtering**. Allow only approved attachment types (including in archives and nested archives). Analyse/sanitise hyperlinks, PDF and Microsoft Office attachments. Quarantine Microsoft Office macros.	Medium	Medium	Medium
Excellent	**Web content filtering**. Allow only approved types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks and free domains.	Medium	Medium	Medium
Excellent	**Deny corporate computers direct internet connectivity**. Use a gateway firewall to require use of a split DNS server, an email server and an authenticated web proxy server for outbound web connections.	Medium	Medium	Low
Excellent	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Low	Low	Low
Very Good	**Server application hardening** especially internet-accessible web applications (sanitise input and use TLS not SSL) and databases, as well as applications that access important (sensitive/high-availability) data.	Low	Medium	Medium
Very Good	**Operating system hardening** (including for network devices) based on a Standard Operating Environment, disabling unneeded functionality (e.g. RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR and WPAD).	Medium	Medium	Low
Very Good	**Antivirus software using heuristics and reputation ratings** to check a file's prevalence and digital signature prior to execution. Use antivirus software from different vendors for gateways versus computers.	Low	Low	Low
Very Good	**Control removable storage media and connected devices**. Block unapproved CD/DVD/USB storage media. Block connectivity with unapproved smartphones, tablets and Bluetooth/Wi-Fi/3G/4G/5G devices.	High	High	Medium
Very Good	**Block spoofed emails**. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use 'hard fail' SPF TXT and DMARC DNS records to mitigate emails that spoof the organisation's domain.	Low	Low	Low
Good	**User education**. Avoid phishing emails (e.g. with links to login to fake websites), weak passphrases, passphrase reuse, as well as unapproved: removable storage media, connected devices and cloud services.	Medium	High	Medium
Limited	**Antivirus software with up-to-date signatures** to identify malware, from a vendor that rapidly adds signatures for new malware. Use antivirus software from different vendors for gateways versus computers.	Low	Low	Low
Limited	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and subsequently leveraged for social engineering. Perform content scanning after email traffic is decrypted.	Low	Low	Low

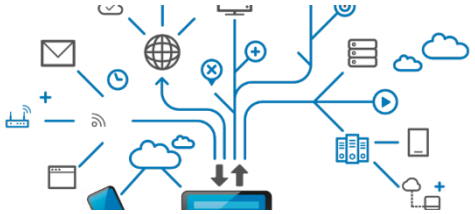
Klasifikacija in definicija premostitvenih ukrepov

ID	Ukrep	Opis in uporaba	Vpliv	Učinek ukrepa
M.1	Polna vidljivost nameščenih aplikacij	Prek standardnega operacijskega okolja zagotoviti popolno vidljivost nameščene programske opreme, dosledno vzdrževati inventar nameščene programske opreme, vpeljati proces upravljanja sprememb	Srednji	Izboljšana vidljivost potencialno ogroženega programja
M.2	Blokiranje nedovoljenega programja	Zagotoviti, da mehanizmi nadzora aplikacij in dovoljenj za dostop do datotečnega sistema blokirajo nedovoljeno programje (pripone .js, .jse, .vbs, .vbe, .wsf itd.)	Srednji	Blokirana zlonamerna koda z nadzorom aplikacij
M.3	Zaščita končnih točk	Uporabiti orodja za zaščito končnih točk in zaščito pred zlonamerno kodo, ki nudijo tudi funkcionalnosti nadzora aplikacij	Srednji	Blokirana zlonamerna koda z nadzorom aplikacij

Premostitveni ukrep je ustrezen za izvedbo:

1. če izboljša izmerjen ali ocenjen vpliv zaznanega kibernetskega incidenta in
2. če dosega ali presega zahtevano stopnjo, saj v nasprotnem primeru stroški premostitvenega ukrepa ne bi upravičili njegovih koristi.

Postopek identifikacije premostitvenih ukrepov



cpe:2.3:a:microsoft:sql_server:2019:*:*:*:*:*:x64:* View CVEs

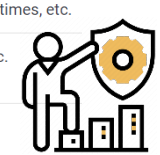
microsoft sql_server

Vuln ID	Summary	CVSS Severity
CVE-2023-23384	Microsoft SQL Server Remote Code Execution Vulnerability **Published:** April 11, 2023; 5:15:18 PM -0400	*V3.1:* 9.8 CRITICAL *V2.0:*(not available)
CVE-2023-21718	Microsoft SQL ODBC Driver Remote Code Execution Vulnerability **Published:** February 14, 2023; 3:15:14 PM -0500	*V3.1:* 7.8 HIGH *V2.0:*(not available)
CVE-2023-21713	Microsoft SQL Server Remote Code Execution Vulnerability **Published:** February 14, 2023; 3:15:14 PM -0500	*V3.1:* 8.8 HIGH *V2.0:*(not available)

Enterprise Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

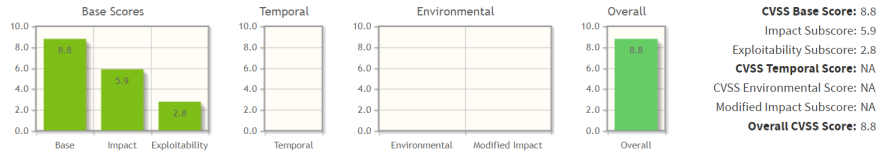
ID	Name	Description
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M1015	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.
M1049	Antivirus/Antimalware	Use signatures or heuristics to detect malicious software.



IT/OT vir → Standardna oznaka vira (CPE) → Ranljivosti (CVE, CWE) → Tehnike napadov (MITRE ATT&CK, CSC, ACSC, interna baza) → Premostitveni ukrepi in strategije (MITRE ATT&CK/D3FEND, CSC, ACSC, priporočila proizvajalcev, interna baza)

Kibernetski incident ali grožnja

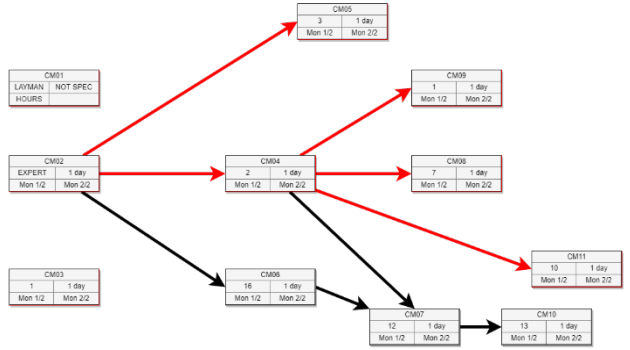
NIST NATIONAL VULNERABILITY DATABASE NVD



Odločitveni model

Dva premostitvena pristopa:

- Premostitvene strategije: zaporedje več premostitvenih ukrepov, ki jih izvedemo v navezavi
- Promostitveni ukrepi: niso del strategije ter se izbirajo in izvajajo neodvisno

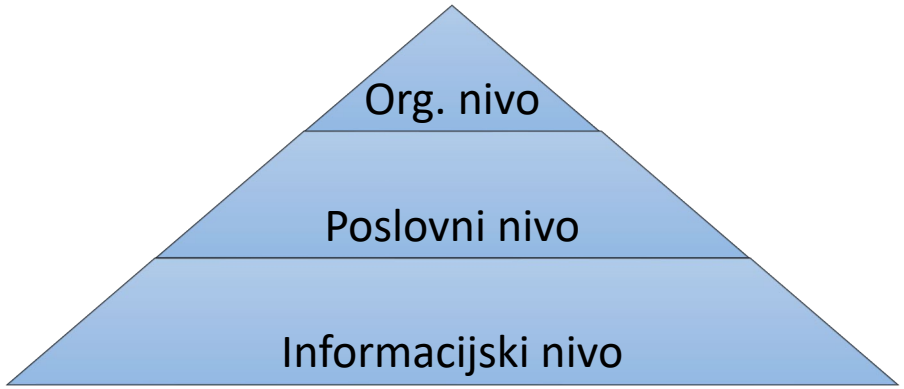


Standardi in priporočila:

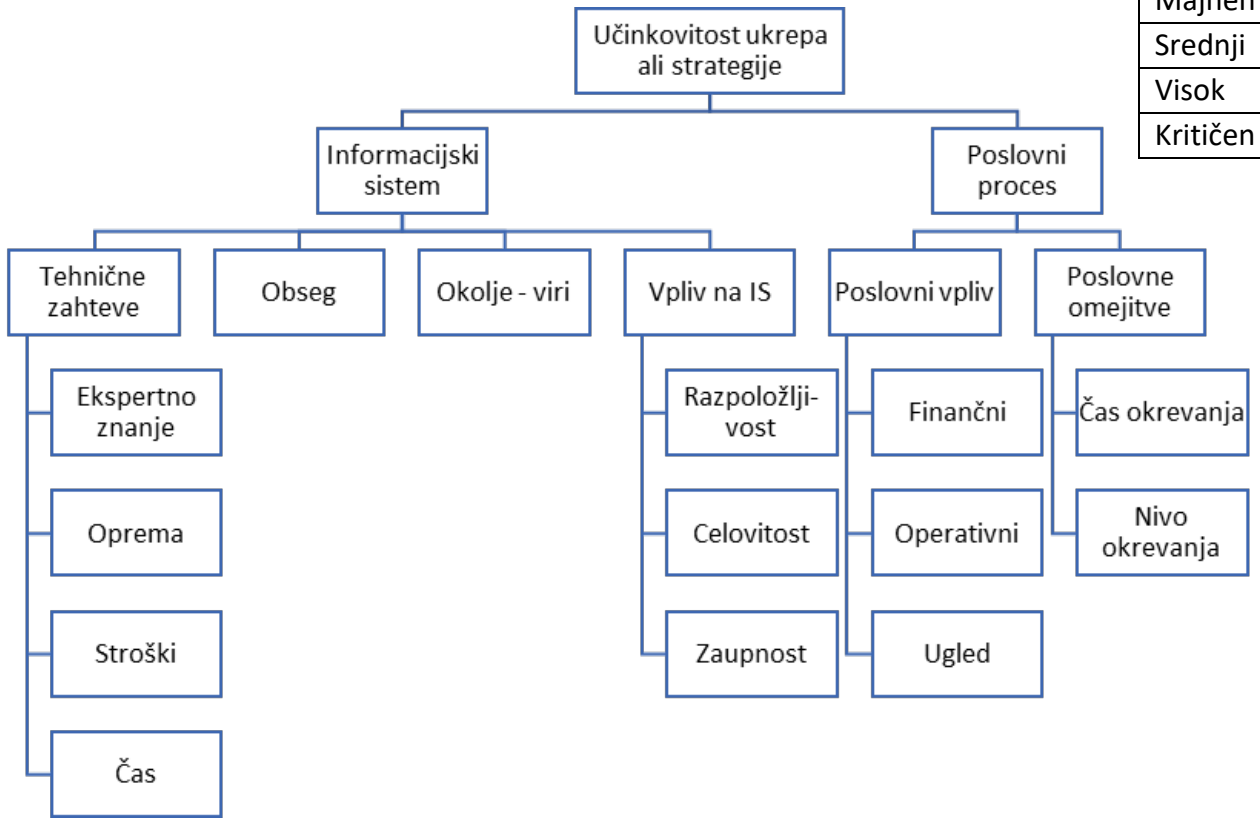
- Priporočila NIST o upravljanju informacijskih varnostnih tveganj
- Splošni kriteriji za varnost IT sistemov po standardu ISO/IEC 15408
- Model CIA – zaupnost, celovitost, razpoložljivost
- Kriteriji za ocenjevanje vplivov infrastrukturnih odpovedi po priporočilih organizacije NESCOR
- Poslovne in organizacijske zahteve
- Tolerančne omejitve ocenjenih organizacijskih tveganj

CSE_i = {T1087.001, T1087.002, T1087.003, T1087.004, T1110.002}

Account Theft = {Local Account Discovery, Domain Account Discovery, Email Account Discovery, Cloud Account Discovery, Password Cracking}



Kriteriji in ocenjevalna lestvica



Kategorija (vpliva)	Ocena CMSS	Barvna klasifikacija
Zanemarljiv	0.0 – 1.0	Zelena
Majhen	1.0 – 4.0	Rumena
Srednji	4.0 – 7.0	Oranžna
Visok	7.0 – 9.0	Svetlo rdeča
Kritičen	9.0 – 10.0	Temno rdeča

1. model: Ocenitev vpliva groženj ali incidentov

2. model: Ocenitev in izbira premostitvenih ukrepov ali strategij

Agregacijski model

$$s^I(A_l) = \sum_{j=1}^{n} w_j s_j^I(A_l)$$

$$s^E(M_k) = \sum_{j=1}^{n} w_j s_j^E(M_k)$$

$$\Delta_w = \min \frac{\left[\sum_{j=1}^{n} \left|w_j - \widetilde{w}_j\right|^P\right]^{1/P}}{\Delta_w^{\max}}$$

glede na

$$s^E(M_k) = \sum_{j=1}^{n} w_j s_j^E(M_k) = C_q$$

$$\sum_{j=1}^{n} w_j = 1$$

$$0 \le w_j \le 1, \forall j = 1, \dots, n$$

Agregacija

Korelacija in veto

$$v^E(M_k) = \gamma \begin{cases} 0 & , \quad s^E(M_k) \le \text{MIAT} \cdot s^I(A_l) \\ \dfrac{s^E(M_k) - \text{MIAT} \cdot s^I(A_l)}{(1 - \text{MIAT}) s^I(A_l)} & , \quad \text{MIAT} \cdot s^I(A_l) < s^E(M_k) < s^I(A_l) \\ 1 & , \quad s^E(M_k) \ge s^I(A_l) \end{cases}$$

$$+(1-\gamma) \begin{cases} 0 & , \quad s^E(M_k) \le C_{\max} - C_\delta \\ \dfrac{s^E(M_k) - (C_{\max} - C_\delta)}{C_\delta} & , \quad C_{\max} - C_\delta < s^E(M_k) < C_{\max} \\ 1 & , \quad s^E(M_k) = C_{\max} \end{cases}$$

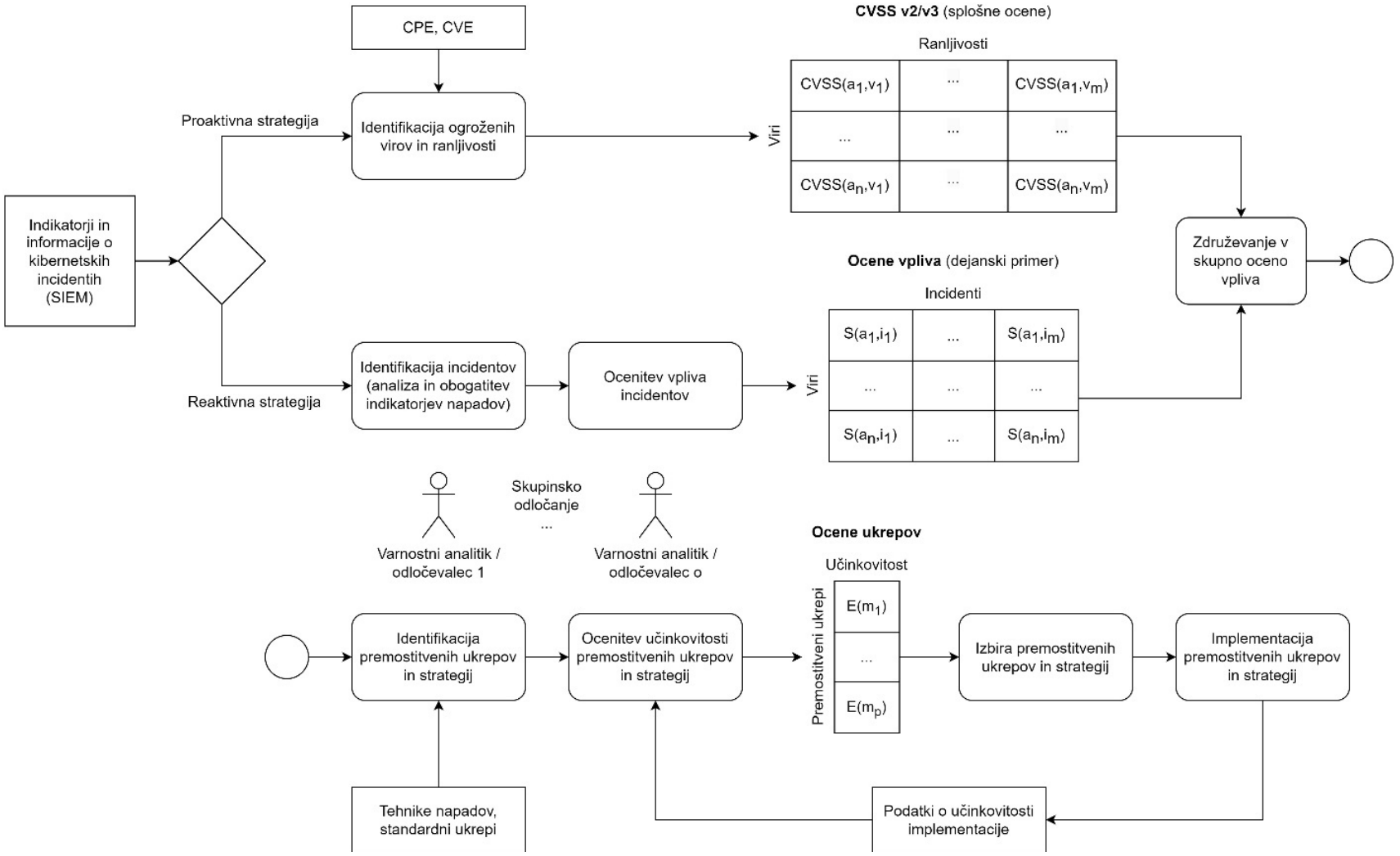
$$S^E(M_k) = s^E(M_k)\left(1 - v^E(M_k)\right)$$

Analiza robustnosti

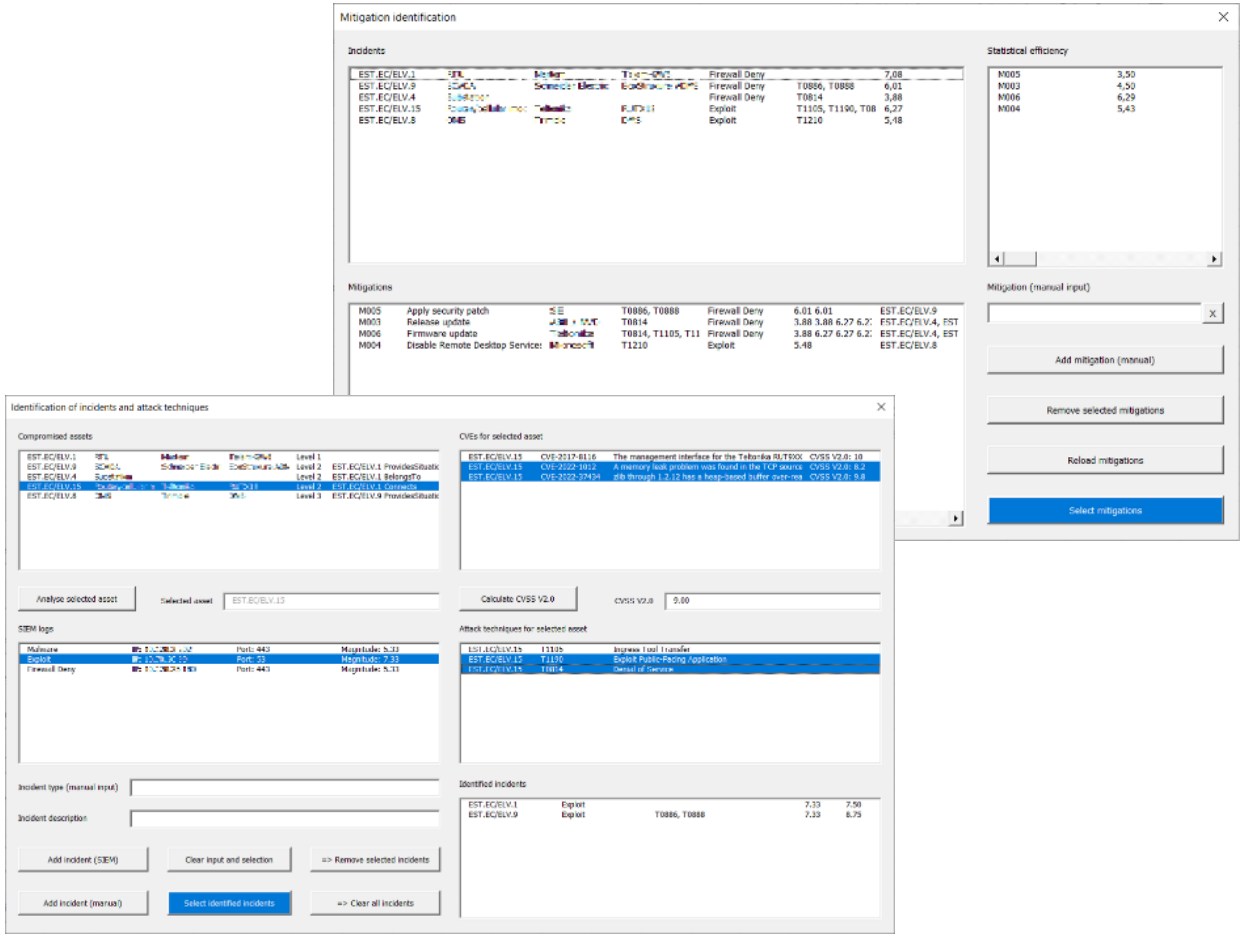
Odločitveni proces – umestitev

	Splošni odločitveni proces	Proces upravljanja tveganj	Proces odzivanja	Implementirani odločitveni proces
Inteligenca	Definicija zahtev Zbiranje podatkov Analiza informacij Identifikacija problema	Določitev konteksta	Opazuj	Zbiranje varnostnih podatkov - integracija s SIEM Obogatitev in analiza indikatorjev napadov Identifikacija incidentov Identifikacija ogroženih virov in ranljivosti
Oblikovanje	Identifikacija alternativ Določitev kriterijev Oblikovanje modela Specifikacija uteži kriterijev	Identifikacija tveganj	Umesti	Identifikacija premostitvenih ukrepov ==> Alternative Specifikacija kriterijev za oceno vpliva incidentov Specifikacija kriterijev za oceno učinkovitosti ukrepov Uteževanje kriterijev za oceno vpliva incidentov Uteževanje kriterijev za oceno učinkovitosti ukrepov
		Analiza tveganj		
Izbira	Modelska rešitev Validacija in testiranje Analiza občutljivosti Načrtovanje implementacije	Ovrednotenje tveganj	Odloči	Ocenitev vpliva incidentov Ocenitev premostitvenih ukrepov in strategij Združevanje ocen vpliva z ocenami CVSS in SIEM Analiza občutljivosti ocene vpliva incidentov Analiza občutljivosti ocene učinkovitosti ukrepov Izbira premostitvenih ukrepov in strategij
Implementacija rešitve		Obravnava tveganj	Ukrepaj	Implementacija premostitvenih ukrepov in strategij

Odločitveni proces – koraki



Odločitveni sistem



Asset ID		EST.EC/ELV.1	EST.EC/ELV.9	EST.EC/ELV.4	EST.EC/ELV.15	EST.EC/ELV.8
Asset type		RTU	SCADA	S	Router/cellular modem	OMS
Asset vendor						
Asset product						
Asset level		Level 1	Level 2	Level 2	Level 2	Level 3
Dependency			EST.EC/ELV.1 ProvidesSituation	EST.EC/ELV.1 BelongsTo	EST.EC/ELV.1 Connects	EST.EC/ELV.9 ProvidesSituation
Incident type		Firewall Deny	Firewall Deny	Firewall Deny	Exploit	Exploit
Attack techniques			T0886, T0888	T0814	T1105, T1190, T0814	T1210
SIEM magnitude	0,10		5,33	5,33	5,33	7,33	7,33
CVSS V2.0	0,10		7,50	8,75		9,33	10,00
System scale	0,05		7,00	6,00	6,00	6,00	5,00
Public safety concern	0,05		6,00	5,00	5,00	5,00	4,00
Workforce safety concern	0,05		5,00	4,00	1,00	4,00	3,00
Ecological concern	0,05		4,00	3,00	3,00	3,00	2,00
Financial impact on utility	0,05		8,00	6,00	6,00	6,00	5,00
Restoration costs	0,05		8,00	6,00	1,00	6,00	5,00
Negative impact on generation capacity	0,05		10,00	8,00	3,00	8,00	6,00
Negative impact on energy market	0,05		9,00	7,00	3,00	7,00	6,00
Negative impact on transmission system	0,05		9,00	7,00	3,00	7,00	6,00
Negative impact on customer service	0,05		7,00	6,00	6,00	6,00	5,00
Destroys goodwill toward utility	0,05		3,00	2,00	2,00	2,00	2,00
Immediate economic damage	0,05		8,00	6,00	6,00	6,00	5,00
Long term economic damage	0,05		7,00	6,00	6,00	6,00	5,00
Privacy loss of stakeholders	0,05		10,00	8,00	4,00	8,00	6,00
Resilience of asset	0,05		6,00	5,00	5,00	5,00	4,00
Relevance of asset	0,05		9,00	7,00	7,00	7,00	6,00
Impact score	1,00		7,08	6,01	3,88	6,27	5,48

Mitigation ID				M005	M003	M006	M004
Mitigation description				Apply security patch	Release update	Firmware update	Disable Remote Desktop Servic
Mitigation source							
Incident type				Firewall Deny	Firewall Deny	Firewall Deny	Exploit
Attack techniques				T0886, T0888	T0814	T0814, T1105, T1190	T1210
Asset ID				EST.EC/ELV.9	EST.EC/ELV.4, EST.EC/ELV.15	EST.EC/ELV.4, EST.EC/ELV.15	EST.EC/ELV.8
Asset type				SCADA	Substation, Router/cellular mod	Substation, Router/cellular mod	OMS
Incident impact score				6,01	5,08	5,67	5,48
Technical requirements	Expertise	0,20	0,25	2,00	4,00	8,00	6,00
	Equipment		0,25	2,00	4,00	8,00	6,00
	Cost		0,25	4,00	4,00	7,00	7,00
	Time		0,25	4,00	5,00	6,00	7,00
Scope	Scope	0,10	1,00	3,00	6,00	7,00	2,00
Environmental	Assets	0,10	1,00	3,00	6,00	6,00	2,00
IS impact	Availability	0,20	0,34	4,00	4,00	6,00	4,00
	Integrity		0,33	4,00	4,00	5,00	4,00
	Confidentiality		0,33	4,00	4,00	5,00	5,00
Business impact	Financial	0,20	0,34	4,00	5,00	3,00	6,00
	Reputation		0,33	5,00	5,00	7,00	6,00
	Operational		0,33	5,00	6,00	9,00	7,00
Business constraints	RTO	0,20	0,50	2,00	3,00	6,00	6,00
	RPO		0,50	2,00	3,00	5,00	8,00
Mitigation score				3,33	4,52	6,18	5,23
Mitigation veto				0,00	0,36	0,25	0,44
Effective mitigation score				3,33	6,50	9,04	7,35
Selected				Yes	Yes	No	No

Zaključek in razprava

- Predstavili smo celovit odločitveni proces za izbiro premostitvenih ukrepov in premostitvenih strategij, s katerimi lahko zmanjšamo vplive kibernetskih incidentov in groženj.
- Gre za enega od vmesnih rezultatov mednarodnega raziskovalnega projekta Horizon 2020 CyberSEAS.
- Metodologija je primerna za uporabo v kateremkoli kompleksnem IT ali IT-OT integriranem okolju, čeprav smo jo prvotno zasnovali za varovanje sistemov elektroenergetske kritične infrastrukture.